IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	George H. Forman	§	Art Unit:	2162
		§		
Serial No.:	10/654,821	§		
		§	Examiner:	Brent S. Stace
Filed:	September 4, 2003	§		
		§		
For:	Determining Point-of-Compromise	§	Atty. Dkt. No.:	200309653-1 (HPC.0329US)
		§		

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDED
APPEAL BRIEF PURSUANT TO 37 C.F.R § 41.37

Sir:

The final rejection of claims 1-7, 9-15, 17-23, and 25-32 is hereby appealed.

I. REAL PARTY IN INTEREST

The real party in interest is the Hewlett-Packard Development Co., LP.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF THE CLAIMS

Claims 1-7, 9-15, 17-23, and 25-32 have been finally rejected and are the subject of this appeal. Claims 8, 16, and 24 have been cancelled.

IV. STATUS OF AMENDMENTS

No amendment after final has been filed.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

Independent claim 1 recites a method for predicting potential points-of-compromise, the method comprising:

> storing a database (Fig. 1:100; Spec., ¶¶ [0021, 0025]) correlating each first member of a first set, wherein each of said first members may be compromised (Fig. 1:CC_1-CC_H; Spec., ¶ [0023]), with each second member of a second set, wherein each of said second members may be a potential point-of compromise (Fig. 1: M_1-M_S; Spec., ¶ [0023]).
>
> recording in said database each interaction of a first member with a second member (Spec., ¶¶ [0021, 0025])
>
> for a given third set of third members, wherein each of said third members is a given compromised first member (Fig. 3:301; Spec., ¶ [0033]) from said database, selecting interactions associating said third members and said second members (Spec., ¶¶ [0034, 0036]);
>
> calculating interaction factors for respective second members that are part of interactions involving the third members, each interaction factor indicating a number of occurrences of interactions involving said third members at a corresponding second member (Fig. 3:319, 325; Spec., ¶¶ [0036-0037]); and
>
> predicting at least one potential point-of-compromise from results of said calculating (Fig. 3:327; Spec., ¶¶ [0037, 0042,0043]).

Independent claim 11 recites a method for identifying possible points-of-compromise, the method comprising:

creating a matrix (Fig. 1:100; Spec., ¶¶ [0021, 0025]) correlating a plurality of at least first items (Fig. 1: CC_1-CC_H; Spec., ¶ [0023]) and second items, each second item representing a potential point-of-compromise (Fig. 1: M_1-M_S; Spec., ¶ [0023]);

logging in said matrix every interactivity involving pairs of said first and second items Spec., ¶¶ [0021, 0025]);

for a given subset of the first items (Fig. 3:301; Spec., ¶ [0033]), extracting from said matrix all interactivities of the first items in said subset with second items (Spec., ¶¶ [0034, 0036]);

tabulating extracted said interactivities according to frequency of said interactivities (Fig. 3:319, 325; Spec., ¶¶ [0036, 0037]); and

assigning a point-of-compromise score to each of said second items that are involved in the extracted interactivities, wherein each said score is indicative of frequency of the extracted interactivities occurring at the corresponding second item (Spec., ¶¶ [0037,0042, 0043]).

Independent claim 17 recites a data storage and data mining process for determining at least one probable point-of-compromise for members of a data set, the process comprising:

in a set of data files (Fig. 1:100; Spec., ¶¶ [0021, 0025]), logging every individual transaction between first members and second members, wherein said first members are subject to compromise (Fig. 1: CC_1-CC_I; Spec., ¶ [0023]) and said second members are each a potential point-of-compromise (Fig. 1: M_1-M_S; Spec., ¶ [0023]).

for a given set of compromised first members, segregating a subset (Fig. 3:301; Spec., ¶ [0033]) of the data files for a predetermined past time period, wherein said subset has at least one of said first members logged therein (Spec., ¶¶ [0034, 0036]);

for each of said second members in said subset, incrementing a corresponding second member tally in response to each said individual transaction associated with each one of said compromised first members, and creating a set of the second member tallies that are associated with respective second members (Fig. 3:319, 325; Spec., ¶¶ [0036-0037]); and

organizing said set of second member tallies according to a predetermined scoring statistic associated with probability of point-of-compromise (Fig. 3:327; Spec., ¶¶ [0037, 0042, 0043]).

Independent claim 18 recites a data storage and data mining system for determining at least one probable point-of-compromise for members of a data set, the system comprising:

means for storing data files (Spec., ¶¶ [0021, 0025]);

means for logging in said data files every individual transaction between first members and second members, wherein said first members are subject to compromise (Fig. 1: CC_1-CC_H; Spec., ¶ [0023]) and said second members are each a potential point-of-compromise (Fig. 1: M_1-M_S; Spec., ¶ [0023]);

for a given set of compromised first members, means for segregating a subset (Fig. 3:301; Spec., ¶ [0033])of the data files for a predetermined past time period, wherein said subset has at least one of said first members logged therein (Spec., ¶¶ [0034, 0036]);

for each of said second members in said subset, means for incrementing a corresponding second member tally in response to each said individual transaction associated with each one of said compromised first members and for creating a set of the second member tallies that are associated with respective second members (Fig. 3:319, 325; Spec., ¶¶ [0036-0037]); and

means for organizing said set of second member tallies according to a predetermined scoring statistic associated with potential as a point-of-compromise (Fig. 3:327; Spec., ¶¶ [0037, 0042, 0043]).

Independent claim 19 recites a method of determining credit card fraud point-of-compromise scores, the method comprising:

correlating issued credit cards (Fig. 1: CC_1-CC_H; Spec., ¶ [0023]) with authorized points-of-use (Fig. 1: M_1-M_S; Spec., ¶ [0023]) such that transactions involving use of a credit card are retrievably logged in a database (Fig. 1:100; Spec., ¶¶ [0021, 0025]);

for a given set of compromised credit cards (Fig. 3:301; Spec., ¶¶ [0033]), extracting from said database all transactions involving use of each of said compromised credit cards (Spec., ¶¶ [0034, 0036]);

for each of said authorized points-of-use involved in at least one of said transactions involving at least one of said compromised credit cards, creating a tally of said transactions for each point-of-use, and incrementing each said tally for each occurrence of transaction involving at least one of said compromised credit cards (Fig. 3:319, 325; Spec., ¶¶ [0036-0037]);

sorting said authorized points-of-use according to the tallies (Fig. 3:327; Spec., ¶ [0037]); and

assigning a score representative of point-of-compromise likelihood to each of said authorized points-of-use according to the respective tally (Spec., ¶¶ [0037, 0042, 0043]).

Independent claim 28 recites a method of doing business comprising:

receiving a set of credit card numbers (Fig. 1: CC_1-CC_H; Spec., ¶ [0023]) and a set of merchants (Fig. 1: M_1-M_S; Spec., ¶ [0023]) authorized to accept said credit cards;

forming a matrix (Fig. 1:100; Spec., ¶¶ [0021, 0025]) of said numbers and said merchants;

logging each use of a card with a merchant as a predetermined data point of said matrix (Spec., ¶¶ [0021, 0025]);

for a given set of compromised credit card numbers (Fig. 3:301; Spec., ¶ [0033]), extracting each related said data point of said matrix (Spec., ¶¶ [0034, 0036]);

incrementing a tally for each merchant associated with each related said data point (Fig. 3:319; Spec., ¶ [0036]); and

sorting said merchants according to the tallies (Fig. 3:325, 327; Spec., ¶¶ [0037]).

Independent claim 29 recites a computer memory comprising:

computer code for compiling a database (Fig. 1:100; Spec., ¶¶ [0021, 0025]) wherein members of a first class (Fig. 1: CC_1-CC_H; Spec., ¶ [0023]) are associated with members of a second class (Fig. 1: M_1-M_S; Spec., ¶ [0023]) in accordance with each interaction of a member of the first class with a member of the second class;

computer code for extracting from said database only those interactions for a predetermined past time period associated with a given subset (Fig. 3:301; Spec., ¶ [0033]) of members of the first class wherein said given subset represents individual compromised members of said first class (Spec., ¶¶ [0034, 0036]); and

computer code for assigning a score to individual members of the second class for each of said interactions extracted wherein said score represents a point-of-compromise probability for each of said individual members of the second class (Fig. 3:319, 325, 327; Spec., ¶¶ [0036-0037, 0042, 0043]).

Independent claim 30 recites:

given a computerized matrix (Fig. 1:100; Spec., ¶¶ [0021, 0025]) of interactivity events between items-of-use (Fig. 1: CC_1-CC_H; Spec., ¶ [0023]), each having a unique first identifier, and points-of-use (Fig. 1: M_1-M_S; Spec., ¶ [0023]), each having a unique second identifier, and a set of compromised said items-of-use, wherein said matrix further comprises a plurality of files, each of said files covering a given time frame for said interactivity events, a method for point-of-compromise scoring comprising:

determining a time-of-first-known-fraud for each said compromised said items-of-use (Spec., ¶ [0031]);

for each said compromised said items-of-use, assigning a suspected date window prior to said time-of-first-known-fraud (Spec., ¶ [0031]);

selecting those ones of said files included in said suspected date window, wherein said compromised said items-of-use are included in said files (Spec., ¶ [0031]);

for each selected file and for each compromised said items-of-use, counting the number of said interactivity events for each of said points-of-use in each said selected file (Fig. 3:319, 325; Spec., ¶¶ [0036-0037]); and

assigning the highest score indicative of point-of-compromise to a highest scoring one of said points-of-use (Fig. 3:327; Spec., ¶¶ [0037, 0042, 0043]).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-3, 9-11, 13, 15, 19-21, 25, and 29 Rejected under § 103 over U.S. Patent No. 6,094,643 (Anderson).

B. Claim 28 Rejected under § 103 over Anderson in view of U.S. Patent No. 5,421,008 (Banning).

C. Claims 17, 18, 31, and 32 Rejected under § 102 over Anderson.

D. Claims 4-7, 12, 14, 22, 23, 26, and 27 Rejected under § 103 over Anderson in View of U.S. Patent No. 5,937,406 (Balabine).

E. Claim 30 Rejected under § 103 over Anderson in View of Balabine and U.S. Patent No. 5,404,507 (Bohm).

VII. ARGUMENT

The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-headings as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Claims 1-3, 9-11, 13, 15, 19-21, 25, and 29 Rejected under § 103 over U.S. Patent No. 6,094,643 (Anderson).

1. Claims 19-21, 25.

Independent claim 19 was rejected as being obvious over Anderson alone. It is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 28, as Anderson does not teach or suggest all elements of claim 19. *See* MPEP § 2143 (8th edition, revision 5), at 2100-129.

Claim 19 recites a method of determining credit card fraud point-of-compromise scores, comprising:

- correlating issued credit cards with authorized points-of-use such that transactions involving use of a credit card are retrievably logged in a database;
- for a given set of compromised credit cards, extracting from said database all transactions involving use of each of said compromised credit cards;
- for each of said *authorized points-of-use* involved in at least one of said transactions involving at least one of said compromised credit cards, creating a tally of said transactions *for each point-of-use*, and incrementing each said tally for each occurrence of transaction involving at least one of said compromised credit cards;
- sorting said *authorized points-of-use* according to *the tallies*; and

- assigning a score representative of point-of-compromise likelihood to each of said *authorized points-of-use* according to the respective tally.

It is significant to note that the focus of the subject matter described in Anderson is different from that of the subject matter of the claimed invention. The focus of Anderson is "for identifying a relatively few suspect counterfeit card transactions from among the massive number of card transactions which occur on a daily basis." Anderson, 1:16-20. According to Anderson, the technique starts by identifying suspicious activity gathered from various financial institutions or by analyzing all activity for a particular time period. Anderson, 3:26-30. From among the massive number of transactions, a small group of transactions that are most suspicious are collected. Anderson, 3:31-36. The suspicious transactions "become the feeder stock for fraud processing." Anderson, 3:51-52. Scores are then applied to both *cards* and *individual transactions* performed with the cards. Anderson, 3:52-55. Based on the scores assigned to the cards and individual transactions, suspect cards are identified and sent to issuing financial institutions for confirmation. Anderson, 4:2-3.

Whereas Anderson is focused on assigning scores to cards and individual transactions for the purpose of identifying individual fraudulent transactions, the claimed invention relates to creating tallies of transactions *for each authorized point-of-use*. The claimed invention also recites *sorting* the *authorized points-of-use* according to the tallies, and assigning a score representative of point-of-compromise likelihood to each of the *authorized points-of-use*. The creation of tallies for authorized points-of-use, sorting of authorized points-of-use according to tallies, and assigning of scores to the authorized points-of-use are clearly not contemplated by Anderson, whose focus is on identifying fraudulent credit cards and fraudulent transactions. Nowhere within Anderson is there any suggestion of creating tallies for authorized points-of-use

such that the authorized points-of-use can be sorted and assigned corresponding scores representative of point-of-compromise likelihood.

In the rejection of claim 19, the Examiner did not provide a specific explanation of what is considered the "authorized points-of-use" recited in claim 19. For the "correlating" element of claim 19 (which correlates issued credit cards with authorized points-of-use), the Office Action cited the following passages of Anderson: column 6, lines 2-6, column 9, lines 53-65. The cited column 6 passage refers to analyzing cards involved in suspicious transactions to determine other transactions that the individual cards were involved in that day. The cited column 9 passage refers to a chaining tool that allows an analyst to review the current day's activity in light of historical activity over the last five days or other cases or points-of-compromise, and to "assess the on-going nature and impact of today's work."

Nowhere within these two cited passages is there any reference to an *authorized point-of-use*. Anderson does refer to merchants, which would be an example of an authorized point-of-use. Yet the Examiner pointedly avoided reference to merchants as being the authorized points-of-use recited in claim 19, for the very basic reason that Anderson clearly does not provide any suggestion that tallies would be calculated for such merchants. In fact, the Examiner has conceded that Anderson fails to disclose sorting merchants according to tallies. *See* 9/28/2006 Office Action at 25 (rejection of claim 28).

As teaching the task of "creating a tally of said transactions for each point-of-use, and incrementing each said tally for each occurrence of transaction involving at least one of said compromised credit cards," the Office Action cited the following passages of Anderson: column 7, line 49-column 8, line 38; column 8, lines 45-60; column 9, lines 13-27; column 9, lines 55-65. The cited passage spanning columns 7 and 8 of Anderson refers to scoring parameters that

are produced for *cards* and *transactions*. There are no scores created for the merchants or other authorized points-of-use. The passage in column 8, lines 45-60, of Anderson cited by the Examiner, refers to scored *transactions* that are grouped into events according to time and geographical region. The cited column 8 passage then refers to analyzing and scoring the events based on individual cards and transactions. The cited passage also refers to selecting transactions for the day and region. However, generating scores for "events" as described in the cited column 8 passage clearly is not the same as producing tallies for *authorized points-of-use*.

The passage in column 9, lines 13-27, of Anderson refers to event scoring parameters that include number of cards with dollar amounts greater than some value, high dollar cards with more than one type of a particular purchase, and number of cards with uses greater than some value. The event scoring parameters clearly do not correspond to tallies of *authorized points-of-use*. The cited passage in column 9, lines 55-65 of Anderson refers to a chaining tool that allows an analyst to review the activity of a current day in view of historical activity, and to assess the on-going nature and impact of a day's work. Again, no suggestion is made of generating tallies for authorized points-of-use.

With respect to the recited element of "sorting said authorized points-of-use according to the tallies" in claim 19, the Examiner cited the following passage of Anderson: column 8, lines 45-60. As discussed above, the scores referred to in this passage are for events. However, there is no sorting of *authorized points-of-use* according to the scores generated for events described in column 8 of Anderson.

Claim 19 further recites assigning a score representative of point-of-compromise likelihood to each of the authorized points-of-use according to the respective tally. In the Office Action, the Examiner cited to various passages of Anderson as disclosing this feature of claim

19. First, the Office Action cited column 6, lines 1-30, of Anderson, which refers to scoring transactions and cards. The cited column 6 passage also notes that the scored transactions are categorized by time and geographical region into smaller groups referred to as events. Based on the scored events, suspect cards are flagged as suspicious and reported to the financial institutions for confirmation. Nowhere in this passage is there any indication or suggestion of assigning a score representative of point-of-compromise likelihood to each of the *authorized points-of-use*.

The Office Action also cited column 5, lines 16-21, as disclosing the score assigning element of claim 19. The passage in column 5 cited by the Examiner refers to starting with a small group of transactions that appear most suspicious, and gathering initial data that is then sifted through a series of filters from the issuer's view. There is no indication or suggestion of assigning a score representative of point-of-compromise likelihood to each of the authorized points-of-use according to the respective tally in this passage of column 5.

The Examiner also cited column 8, lines 45-60, of Anderson. However, as noted above, this passage refers to creating scores for events; there clearly is no suggestion here of assigning a score to each authorized point-of-use as recited in claim 19. Finally, the Examiner cited two passages in column 9 of Anderson, including the passages in lines 13-27 and 54-65. The first cited passage in column 9 refers to event scoring parameters, which are scoring parameters for events, not for authorized points-of-use. The second passage of column 9 cited by the Examiner refers to an analyst reviewing a current day's activity in light of historical activity to assess the nature and impact of a particular day's work. Again, no suggestion is made of assigning a score representative of point-of-compromise likelihood to each of the authorized points-of-use according to the respective tally.

The Examiner argued that Anderson discloses all elements of claim 19 except for "logged in a database." 9/28/2006 Office Action at 15. However, this is not the only shortcoming of Anderson; Anderson also fails to teach or suggest the "creating a tally" element, "sorting said authorized points-of-use" element, and "assigning a score" element recited in claim 19. Since there is no objective evidence that would have provided a suggestion, whether implicit or explicit, of a modification of Anderson to achieve the claimed invention, it is respectfully submitted that the Examiner has failed to establish a *prima facie* case of obviousness with respect to claim 19 and its dependent claims.

In view of the foregoing, reversal of the final rejection of the above claims is respectfully requested.

2. Claims 1-3, 9, 10.

Independent claim 1 was also rejected as being obvious over Anderson alone. It is respectfully submitted that a *prima facie* case of obviousness has also not been established with respect to claim 1 for at least the reason that Anderson does not teach or suggest all elements of claim 1.

Claim 1 recites a method that includes calculating interaction factors for respective second members (which are potential points-of-compromise) that are part of interactions involving third members (which are compromised first members), where each interaction factor indicates a number of occurrences of interactions involving the third members at a corresponding second member. Thus, claim 1 specifically teaches the calculating of interaction factors indicating numbers of occurrences of interactions for respective potential points-of-compromise. Claim 1 further recites predicting at least one potential point-of-compromise from results of the calculating.

In the Office Action, the Examiner pointed specifically to column 8, lines 15-20, as teaching the interaction factors of claim 1. *See* 9/28/2006 Office Action at 3 ("Particular attention should be brought to Anderson col. 8, lines 15-20."). Column 8, lines 15-20 of Anderson refers to the following parameters: number of days card appears in the POS five-day table, total number of successful transactions in the history table, total number of successful transactions for greater than two hundred dollars in the POS five-day table, and total dollar amount of successful transactions by card in the POS five-day table. However, the parameters of the cited column 8 passage are scoring parameters that score "all cards and transactions." Anderson, 7:50-51. The cited passage does not disclose interaction factors for respective potential points-of-compromise that are part of interactions involving compromised first members (third members).

Thus, in addition to not disclosing the claimed subject matter conceded by the Examiner as not appearing in Anderson, it is noted that Anderson further fails to teach or suggest teach or suggest the claim features discussed above. No objective evidence exists of a modification of Anderson to achieve the claimed invention. Therefore, it is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 1 and its dependent claims.

Reversal of the final rejection of the above claims is respectfully requested.

3. Claims 11, 13, 15.

Independent claim 11 was also rejected as being obvious over Anderson alone. Claim 11 recites a method that includes the following tasks:

- for a given subset of the first items, extracting from the matrix all interactivities of the first items in the subset with second items;

- tabulating extracted said interactivities according to frequency of said interactivities;
- assigning a point-of-compromise score to each of said second items (where each second item represents a potential point-of-compromise) that are involved in the extracted interactivities, wherein each of said scores is indicative of frequency of the extracted interactivities occurring at the corresponding second item (potential point-of-compromise).

Thus, claim 11 specifically recites assigning point-of-compromise scores to each of the potential points-of-compromise (second items) that are involved in the extracted interactivities, where each score is indicative of frequency of the extracted interactivities occurring at the corresponding second item. In the Office Action, the Examiner referred in particular to column 6, lines 1-30, of Anderson as disclosing this feature of claim 11. 9/28/2006 Office Action at 4. The cited passage in column 6 of Anderson refers to scoring transactions that can be grouped into smaller groups referred to as events. Scoring events, which are groups of transactions, clearly is different from assigning scores to potential points-of-compromise, as recited in claim 11.

Thus, in addition to the subject matter conceded by the Examiner as not being taught by Anderson, Anderson further fails to teach or suggest the assigning task of claim 11. Therefore, a *prima facie* case of obviousness has not been established with respect to claim 11.

In view of the foregoing, reversal of the final rejection of the above claims is respectfully requested.

4. Claim 29.

Independent claim 29 was also rejected as being obviousness over Anderson alone. Claim 29 recites a computer memory that comprises computer code for assigning a score to individual members of the second class for each of the interactions extracted, where the score represents a point-of-compromise probability for each of the individual members of the second class.

With respect to the rejection of claim 29, in addition to the passages cited against the other claims (and discussed above), the Examiner focused specifically on the passage of Anderson at column 7, line 49-column 8, line 38. 9/28/2006 Office Action at 5. As discussed above, the parameters listed in Table 1 in the cited passage of Anderson are scoring parameters that score cards and transactions. The scoring parameters clearly do not represent a point-of-compromise probability for each of the individual members of the second class.

Therefore, in addition to the subject matter conceded by the Examiner as missing from Anderson, Anderson also clearly fails to teach or suggest the computer code for assigning a score as recited in claim 29. Therefore, a *prima facie* case of obviousness has not been established with respect to claim 29.

Reversal of the final rejection of the above claim is respectfully requested.

B. Claim 28 Rejected under § 103 over Anderson in view of U.S. Patent No. 5,421,008 (Banning).

1. Claim 28.

Independent claim 28 was rejected as being obvious over Anderson in view of Banning.

Claim 28 recites a method that includes incrementing a tally for each merchant associated with each related said data point, and sorting the merchants according to the tallies. With respect to the incrementing task, the Examiner cited the following passages of Anderson: column 7, line

49-column 8, line 38; column 8, lines 45-60; column 9, lines 13-27; column 9, lines 55-65. The cited passage in columns 7 and 8 refers to scoring parameters for cards and transactions; there is absolutely no suggestion whatsoever that such scoring parameters are tallies for *merchants*.

The cited passage in column 8, at lines 45-60, of Anderson refers to grouping transactions into events, which are analyzed and scored. Again, the analysis and scoring of the events clearly does not produce tallies for *merchants*, as recited in claim 28.

The passage in column 9, at lines 13-27, of Anderson refers to scoring parameters for *events*, not for *merchants*. The passage in column 9, at lines 55-65, of Anderson, refers to a chaining tool that allows an analyst to review the current day's activity in light of historical activity to assess the on-going nature and impact of a day's work. No suggestion is provided of creating tallies for merchants, as recited in claim 28.

Thus, in view of the erroneous application of Anderson to the incrementing task of claim 28, the obviousness rejection is defective.

Moreover, the Examiner conceded that Anderson does not disclose, *inter alia,* sorting the merchants according to the tallies. 9/28/2006 Office Action at 25 (the Examiner also conceding that Anderson fails to disclose forming a matrix, and logging each use of a card with a merchant as a predetermined data point of the matrix).

With respect to the task of sorting the merchants according to the tallies, the Examiner cited Banning, and in particular, to column 9, lines 1-6 of Banning. Note that Banning describes a system for interactive graphical construction of a database query in storing of query object links. The cited passage in column 9 of Banning relates to elements of a database query language (SQL) query. As noted by Banning, an SQL query establishes a set of eight basic data structures. The cited passage in column 9 of Banning refers to element (7) and (8). Element (7) is an

OrderBy clause in the SQL query to allow the definition of ascending order or descending order of listing of a column name of a relational table. Element (8) of the SQL query is a DistinctFlag that tracks the state of a DISTINCT key word. There is absolutely no suggestion provided in Banning of sorting merchants according to tallies that are produced for corresponding merchants. Therefore, the hypothetical combination of Anderson and Banning clearly does not teach or suggest claim 28.

Moreover, no motivation or suggestion existed to combine the teachings of Anderson and Banning. Anderson describes detecting counterfeit financial card fraud, whereas Banning describes providing graphical queries and direct manipulation of a database. The disparate teachings of Anderson and Banning clearly do not relate to each other, and a person of ordinary skill in the art clearly would not have been motivated to combine the teachings of Anderson and Banning to achieve the claimed subject matter.

In view of the foregoing, it is clear that a *prima facie* case of obviousness has not been established with respect to claim 28. Therefore, reversal of the final rejection of the above claim is respectfully requested.

C. Claims 17, 18, 31, and 32 Rejected under § 102 over Anderson.

1. Claims 17, 18, 31, 32.

Claim 17 recites logging every individual transaction between first members and second members, where the first members are subject to compromise and the second members are each a potential point-of-compromise. Claim 17 further recites that for each of said second members (which are potential points-of-compromise) in a subset, a separate second member tally is incremented in response to each individual transaction associated with each one of the

compromised first members, and a set is created of the second member tallies that are associated with respective second members (which are potential points-of-compromise).

The Examiner cited the following passages of Anderson as disclosing the incrementing of second member tallies: column 7, line 49-column 8, line 38; column 8, lines 45-60; column 9, lines 13-27; column 9, lines 55-65. 9/28/2006 Office Action at 8. These cited passages refer to creating scores for all cards and transactions based on standardized scoring parameters. Anderson, 7:50-51. Moreover, Anderson teaches that the scored transactions are categorized by time and geographic region into smaller groups referred to as events. Anderson, 8:42-44. Importantly, note that events refer to groups of transactions. Anderson further states that the events are scored by transactional attributes carried with a card and in view of other transactions in a particular event. Anderson, 9:5-7. The events are scored using event scoring parameters. Anderson, 9:13-15. The scored events are then analyzed to identify fraudulent patterns. Anderson, 9:44-46.

Thus, the scores that are computed by Anderson are scores for cards, transactions, or events (which are groups of transactions). In contrast, the tallies incremented according to claim 17 are tallies for each of second members in a subset, where the second members are each a *potential point-of-compromise*.

The Examiner argued that the claims and the specification of the present application "do not limit 'members' as not meaning cards, transactions, or events." 9/28/2006 Office Action at 2. Appellant respectfully disagrees, as claim 17 specifically recites that the second members are each a potential point-of-compromise. Thus, the second-member tally that is incremented in response to each of the individual transactions associated with each of the compromised first members is for a potential point-of-compromise. Also, the created set of second-member tallies

are associated with respective points-of-compromise, according to claim 17. Claim 17 further notes that the second-member tallies (for respective potential points-of-compromise) are organized according to predetermined scoring statistics associated with the probability of point-of-compromise.

The parameters calculated for cards, transactions, and events as taught by Anderson clearly do not disclose the second-member tallies of claim 17. Therefore, claim 17 is not anticipated by Anderson.

Independent claim 18 is similarly allowable. Dependent claims of claims 17 and 18 are also allowable for at least the same reasons.

Therefore, reversal of the final rejection of the above claims is respectfully requested.

D. Claims 4-7, 12, 14, 22, 23, 26, and 27 Rejected under § 103 over Anderson in View of U.S. Patent No. 5,937,406 (Balabine).

1. Claims 4-6.

In view of the defective rejection of claim 1 over Anderson, it is respectfully submitted that the rejection of dependent claim 4 over Anderson and Balabine is also defective.

Moreover, the Examiner conceded that Anderson fails to disclose dividing the database into a plurality of separately retrievable files, where each of the files is characterized by a predetermined time frame bounding interactions between the first members and the second members. 9/28/2006 Office Action at 18. However, the Examiner cited Balabine as disclosing the missing subject matter. *Id.*

Appellant respectfully submits that Balabine clearly does not disclose or suggest the claimed subject matter that is missing from Anderson. The Examiner cited various passages in columns 7 and 8 of Balabine as disclosing the subject matter of claim 4. The cited passages refer

to a Basic Extension Module (BEM) that is part of a file system interface of a computer. In the cited passages, Balabine states that the BEM provides a one-to-one mapping of a file in a file system into a collection of database objects. Balabine also notes that the BEM emulates a file system by encapsulating a collection of database tables, and presenting them to an application as file system objects. The cited passages also note that each file object includes various attributes. Also, the cited passages of Balabine refer to different file system interface extension modules that may be resident and operative at the same time to provide access to two or more different databases simultaneously or to access different information within the same database or to provide a different interpretation of the same database object. Moreover, the cited passages of Balabine refer to using the appropriate extension modules to allow software developers to enable database-unaware applications to retrieve information stored in a database.

There is absolutely no suggestion whatsoever in Balabine of dividing a database into a plurality of separately retrievable files, where each file is characterized by a predetermined time frame bounding interactions between the first members and the second members. Anderson similarly fails to teach or suggest the subject matter, as conceded by the Examiner. Therefore, the hypothetical combination of Anderson and Balabine clearly does not teach or suggest all elements of claim 4 (and its dependent claims).

Reversal of the final rejection of the above claims is respectfully requested.

2. Claims 7, 14.

In view of the defective rejection of claim 1 over Anderson, it is respectfully submitted that the rejection of dependent claim 7 over Anderson and Balabine is also defective. Moreover, the Examiner conceded that Anderson fails to disclose the segregating task of claim 7. The

subject matter of claim 7 recites segregating correlated first members and second members into a plurality of data files, where the data files are identifiable by a predetermined common characteristic of at least one predetermined particular characteristic of a selected one of the first members and second members. The Examiner cited Balabine as disclosing the claimed subject matter that is not disclosed by Anderson.

The Examiner cited various passages in columns 7 and 8 of Balabine, and cited Figures 5A-5C of Balabine, as disclosing the claimed subject matter. The cited passages refer to the basic extension module that provides a one-to-one mapping of a file in a file system into a collection of database objects. The cited passages also refer to the basic extension module emulating a file system by encapsulating a collection of database tables and presenting them to an application as file system objects. Also, the cited passages refer to attributes of a file object. In addition, the cited passages refer to employing appropriate extension modules to allow software developers to enable database-unaware applications to retrieve information stored in a database. Also, the cited passages refer to mapping portions of a database to a file system representation by selecting database tables and rows as desired, and by designating the type of file system object to which each selected table and row corresponds. The cited passages also refer to using different extension modules to access different databases or different information within the same database simultaneously. The cited passages also refer to a single extension module that is capable of presenting the same information in multiple different formats, as different types of file system objects. Figure 5C shows a table of customers, including names, addresses, and IDs that can be presented as a single file system object. However, nowhere within the cited passages of Balabine is there any suggestion of segregating correlated first members (which may be compromised) with second members (which are potential points-of-compromise) into a plurality

of data files, where the data files are identifiable by a predetermined common characteristic of at least one predetermined particular characteristic of a selected one of the first members (that are subject to compromise) and second members (that are potential points-of-compromise).

Anderson also fails to teach or suggest such segregation. Therefore, the hypothetical combination of Anderson and Balabine does not teach or suggest all elements of claim 7.

In view of the foregoing, reversal of the final rejection of the above claim is respectfully requested.

3. Claims 12, 23, 26, 27.

In view of the defective obviousness rejection of base claims 11 and 19 over Anderson alone, it is respectfully submitted that the obviousness rejection of dependent claims 12, 23, 26, and 27 over Anderson and Balabine is also defective. Therefore, reversal of the final rejection of the above claim is respectfully requested.

4. Claim 22.

In view of the defective obviousness rejection of base claim 19 over Anderson alone, it is respectfully submitted that the obviousness rejection of claim 22 over Anderson and Balabine is also defective. Moreover, claim 22 recites that the database comprises a plurality of files, wherein each of the files is characterized by a given time frame bounding the transactions logged. Claim 22 is further allowable for reasons similar to those of claim 4, discussed above. Therefore, reversal of the final rejection of the above claim is respectfully requested.

E. Claim 30 Rejected under § 103 over Anderson in View of Balabine and U.S. Patent No. 5,404,507 (Bohm).

1. Claim 30.

Independent claim 30 was rejected as being obvious over Anderson, Balabine, and Bohm. The obviousness rejection was premised on the defective reading of a claim element of claim 30 onto Anderson, namely the claimed feature of counting the number of the interactivity events for each of the points-of-use in the selected file. In view of the misapplication of Anderson to claim 30, it is respectfully submitted that the hypothetical combination of Anderson, Balabine, and Bohm does not teach or suggest all elements of claim 30. Therefore, a *prima facie* case of obviousness has not been established with respect to claim 30.

Reversal of the final rejection of the above claim is respectfully requested.

VIII. CONCLUSION

In view of the foregoing, reversal of all final rejections and allowance of all pending claims is respectfully requested.

Respectfully submitted,

Date: August 17, 2009

/Dan C. Hu/

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
1616 South Voss Road, Suite 750
Houston, TX 77057-2631
Telephone: (713) 468-8880
Facsimile: (713) 468-8883

APPENDIX OF APPEALED CLAIMS

The claims on appeal are:

1. A method for predicting potential points-of-compromise, the method comprising:

storing a database correlating each first member of a first set, wherein each of said first members may be compromised, with each second member of a second set, wherein each of said second members may be a potential point-of compromise;

recording in said database each interaction of a first member with a second member;

for a given third set of third members, wherein each of said third members is a given compromised first member from said database, selecting interactions associating said third members and said second members;

calculating interaction factors for respective second members that are part of interactions involving the third members, each interaction factor indicating a number of occurrences of interactions involving said third members at a corresponding second member; and

predicting at least one potential point-of-compromise from results of said calculating.

2. The method as set forth in claim 1 said selecting further comprising:

for each of said third members, including each said interaction found for a predetermined past time period.

3. The method as set forth in claim 2 wherein each said predetermined past time period is determined individually from a given time-of-first-known-fraud for each of said third members.

4. The method as set forth in claim 3 wherein said storing and said recording further comprises:

dividing said database into a plurality of separately retrievable files, wherein each of said files is characterized by a predetermined time frame bounding interactions between said first members and said second members.

5. The method as set forth in claim 4 wherein for each of said third members, each said time-of-first-known-fraud and said predetermined past time frame are used to filter out those separately retrievable files not within said predetermined past time period from said selecting.

6. The method as set forth in claim 4 wherein said separately retrievable files are created using identifier features of said second members suited to maximizing data compression.

7. The method as set forth in claim 1, said storing further comprising:

segregating correlated first members and second members into a plurality of data files, wherein said files are identifiable via a predetermined common characteristic of at least one predetermined particular characteristic of a selected one of said first members and said second members.

9. The method as set forth in claim 1, said predicting further comprising:

listing all second members associated in said selecting as a potential point-of-compromise with a score based upon the interaction factors.

10. The method as set forth in claim 9, said predicting further comprising:

adjusting each said score by a common factor associated with each said second member to normalize the scores.

11. A method for identifying possible points-of-compromise, the method comprising:

creating a matrix correlating a plurality of at least first items and second items, each second item representing a potential point-of-compromise;

logging in said matrix every interactivity involving pairs of said first and second items;

for a given subset of the first items, extracting from said matrix all interactivities of the first items in said subset with second items;

tabulating extracted said interactivities according to frequency of said interactivities; and

assigning a point-of-compromise score to each of said second items that are involved in the extracted interactivities, wherein each said score is indicative of frequency of the extracted interactivities occurring at the corresponding second item.

12. The method as set forth in claim 11 further comprising:

sorting said matrix into a plurality of data files such that in each of said files one of said first and second items has a predetermined unique.

13. The method as set forth in claim 11 further comprising:

limiting said extracting to a predetermined past time frame.

14. The method as set forth in claim 12 wherein each of said files is associated with a common structure or characteristic of at least one of said first and second items.

15. The method as set forth in claim 11 wherein each said extracted interactivity is a data pair further comprising a first identifier representative of a compromised first item and an interactivity situation identifier.

17. A data storage and data mining process for determining at least one probable point-of-compromise for members of a data set, the process comprising:

in a set of data files, logging every individual transaction between first members and second members, wherein said first members are subject to compromise and said second members are each a potential point-of-compromise;

for a given set of compromised first members, segregating a subset of the data files for a predetermined past time period, wherein said subset has at least one of said first members logged therein;

for each of said second members in said subset, incrementing a corresponding second member tally in response to each said individual transaction associated with each one of said compromised first members, and creating a set of the second member tallies that are associated with respective second members; and

organizing said set of second member tallies according to a predetermined scoring statistic associated with probability of point-of-compromise.

18. A data storage and data mining system for determining at least one probable point-of-compromise for members of a data set, the system comprising:

means for storing data files;

means for logging in said data files every individual transaction between first members and second members, wherein said first members are subject to compromise and said second members are each a potential point-of-compromise;

for a given set of compromised first members, means for segregating a subset of the data files for a predetermined past time period, wherein said subset has at least one of said first members logged therein;

for each of said second members in said subset, means for incrementing a corresponding second member tally in response to each said individual transaction associated with each one of said compromised first members and for creating a set of the second member tallies that are associated with respective second members; and

means for organizing said set of second member tallies according to a predetermined scoring statistic associated with potential as a point-of-compromise.

19. A method of determining credit card fraud point-of-compromise scores, the method comprising:

correlating issued credit cards with authorized points-of-use such that transactions involving use of a credit card are retrievably logged in a database;

for a given set of compromised credit cards, extracting from said database all transactions involving use of each of said compromised credit cards;

for each of said authorized points-of-use involved in at least one of said transactions involving at least one of said compromised credit cards, creating a tally of said transactions for each point-of-use, and incrementing each said tally for each occurrence of transaction involving at least one of said compromised credit cards;

sorting said authorized points-of-use according to the tallies; and

assigning a score representative of point-of-compromise likelihood to each of said authorized points-of-use according to the respective tally.

20. The method as set forth in claim 19 wherein said extracting is limited to a predetermined time period range of past transactions.

21. The method as set forth in claim 19 wherein each said score is normalized via a characteristic related to point-of-use.

22. The method as set forth in claim 19 wherein said database comprises a plurality of files wherein each of said files is characterized by a given time frame bounding said transactions logged.

23. The method as set forth in claim 22 wherein each of said plurality of files is sortable by identifier data representative of subsets of credit card numbers.

25. The method as set forth in claim 20 wherein said predetermined time period range of past transactions is based upon a given suspected time-of-compromise window prior to a time-of-first-known-fraud for each said credit card.

26. The method as set forth in claim 22 wherein said files comprise a matrix of data compressed identifier pairs wherein each of said pairs includes a credit card identifier and a point-of-use situation identifier.

27. The method as set forth in claim 26 further comprising providing a first database comprising a relational data pair relating said point-of-use situation identifier and said credit card identifier, and a second database correlating each said point-of-use situation identifier to a physical said point-of-use.

28. A method of doing business comprising:

receiving a set of credit card numbers and a set of merchants authorized to accept said credit cards;

forming a matrix of said numbers and said merchants;

logging each use of a card with a merchant as a predetermined data point of said matrix;

for a given set of compromised credit card numbers, extracting each related said data point of said matrix;

incrementing a tally for each merchant associated with each related said data point; and

sorting said merchants according to the tallies.

29. A computer memory comprising:

computer code for compiling a database wherein members of a first class are associated with members of a second class in accordance with each interaction of a member of the first class with a member of the second class;

computer code for extracting from said database only those interactions for a predetermined past time period associated with a given subset of members of the first class wherein said given subset represents individual compromised members of said first class; and

computer code for assigning a score to individual members of the second class for each of said interactions extracted wherein said score represents a point-of-compromise probability for each of said individual members of the second class.

30. Given a computerized matrix of interactivity events between items-of-use, each having a unique first identifier, and points-of-use, each having a unique second identifier, and a set of compromised said items-of-use, wherein said matrix further comprises a plurality of files, each of said files covering a given time frame for said interactivity events, a method for point-of-compromise scoring comprising:

determining a time-of-first-known-fraud for each said compromised said items-of-use;

for each said compromised said items-of-use, assigning a suspected date window prior to said time-of-first-known-fraud;

selecting those ones of said files included in said suspected date window, wherein said compromised said items-of-use are included in said files;

for each selected file and for each compromised said items-of-use, counting the number of said interactivity events for each of said points-of-use in each said selected file; and

assigning the highest score indicative of point-of-compromise to a highest scoring one of said points-of-use.

31. The data storage and mining process of claim 17, wherein incrementing each second member tally comprises incrementing a corresponding count of a number of occurrences of transactions involving the compromised first members at the corresponding second member.

32. The data storage and data mining system of claim 18, wherein each second member tally comprises a count of a number of occurrences of transactions involving the third members at the corresponding second member.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.